A Brief History of Mathematics

The **main** branches of maths are *Geometry (Space), Number (Counting), Algebra (Processes), Analysis (Continuity and Convergence) and Algorithms (Computation).* How old is maths? The oldest **pierced** object was a wolf's tooth in Austria, 300,000 BC (Part of a necklace). 7,000 BC: Sophisticated nets: *knots*, *mesh*. They solved basic problems: Making Knots (Geometry), Iteration.

Some stage: 3,4,5 right angled triangle found. $3^2+4^2=5^2$, or $(m^2-n^2)+(2mn)^2=(m^2+n^2)^2$. Pythagoras' theorem had a consequence *Pythagoras'* hated — $\sqrt{2}$ is not a rational number; there are no integers a,b such that $\sqrt{2} = {}^a/_b$. *Simple* proof: a = whole number. Then a^2 is even if and only if a is even. *Suppose* $\sqrt{2} = {}^a/_b$ (a,b have no *common factor* — if they do have, cancel it). Then $a^2=2b^2$. So a^2 is even, a is even. Let a=2c; so $4c^2=2b^2$; $b^2=2c^2$. So b is even, **no** common factor. Why did P hate it — (Story: he *drowned* an apprentice who told about it) mystical belief universe could be reduced to numbers. We know $\sqrt{2}$ has an *infinite non-repeating decimal expansion* (If it repeated, it would be rational).

How to handle **infinite** processes: Analysis. 380BC (Athens defeated Persia) — 330BC (Athens started fighting Sparta). *Height* of Athenian culture. Centre for culture: Alexandria. Euclid: 365-300BC. Systematic account of Geometry. Influential till 19th century. Started with **assumptions**, **postulates** and **axioms**. Derived consequences using constructions and proofs. One of his postulates, the parallel postulate: Given a line L and a point B there exists (B not on L) exactly one line L' through B and which does *not* meet L.

Archimedes (Eureka): Estimated π. Appolonius: Conic Sections: circles, ellipses, hyperbolas. Eratostheres: 276-197BC. Estimated **circumference** of Earth. 415AD: Hyparia, female mathematician & philosopher.

Number and Algebra

Greek & Roman number system was not adapted for calculation. Great invention: number 0 (Hindus, 200BC). **Basic** Arabic number system. Emphasis because 0 is trivial — seems silly. But essential for calculation. Maths is often concerned with getting simple things right. Two aspects of maths: (1) *Solving difficult problems*. Fermat's last theorem: fuss - thought about it for 7 years. (2) *Making difficult things easy*. Means finding right language for explanation, also notation. Historically, (2) is more important in **applications**. Example: We all use graphs of functions (Descartes, 17th century).

Arabs developed the *number* system, taken up in Europe (15th century) leading to book keeping, and so making money. **Astronomy**. Copernicus, Tycho Brahe (observations), Kepler's laws: (I) Planets move in ellipses with the sun as focus. (II) Distances and length of year. (III) Time to traverse an angle.

Newton’s 3 laws followed from the **inverse** square law for gravitation, F = $^{Gm_1m_2}/_{r^2}$ (*Attraction*). Developed with <u>Lcabric</u>, calculus. Maths develops **furiously** and **increasingly**.

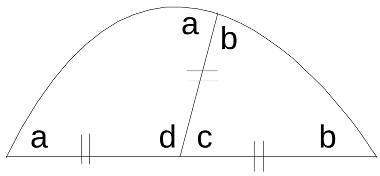
One other major revolution was *non-Euclidean geometry* (Early 19th century). Modern revolution: interaction with computers. People say computers are wonderful — they predict weather, etc. In fact, they do **fast calculations** in mathematical models. Often, new developments of computer calculation have used new mathematics i.e. *new* algorithms (better underlying maths, bigger and faster computers).

Recent revolution, still working out, is **symbolic** calculation (Computer algebra, Maple). But computers are *good at doing algorithms*. Not so good (as yet) at <u>proving</u> theorems and even worse at formulating theorems. (Theorem = **significant** mathematical fact).

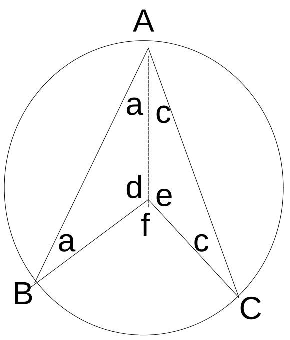
Fermat’s last theorem (17th century): Can you find integers x, y, z such that $x^3+y^3=z^3$, or $x^n+y^n=z^n$, $n\geq3$. Andrew Wiles proved it could **not** happen recently. Proof uses enormous apparatus. In fact he proved a more general and important result. There exists many unsolved problems, e.g. **cuboid** problem: find a rectangular block, all of whose edges face diagonals; main diagonals are *integers*.

Computers don’t help in *formulating questions*, and help only in searching for examples up to limits. Proofs have 3 functions: (1) **Verification** that B follows from A (Conclusions from Assumptions). (2) **Showing** surprising things are true. (3) **Explanation**.

<u>Some Basic Geometry</u>



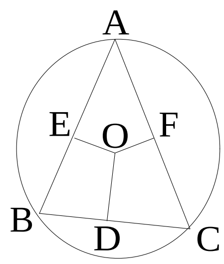
Assume **Pons Asinorum:** In an isosceles triangle, the *base angles* of an isosceles triangle are equal. Prove the angle in a semicircle is 90°. A: Split the triangle in the semicircle into 2 isosceles triangles. 2a+d=180°; 2b+e=180°. Add giving 2a+d+2b+e=360°. As d+e=180°, then 2a+2b=180°, a+b=90°. QED.



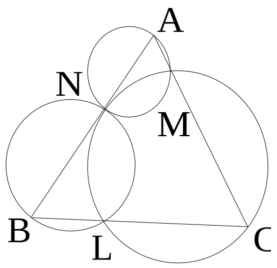
To prove that a chord which **bisects** a diameter is perpendicular to it, use similar triangles and *substitution* as above. To prove that the angle at the centre is <u>double</u> the angle at the circumference, proceed as follows: join OA and name some angles. 2a+d=180°; 2c+e=180°. 2a+2c+d+e=360°; 2(a+c)=360°-(d+e); 2(a+c)=f. QED. A **standard** question in maths is: If A implies B, does B imply A? Method for this example: Find a point A’ on BA such that A’ is not at B, but OA’=OB. Want to *prove* A’=A. By the previous result, Angle BOC=2×BA’C. <u>Given</u> Angle BOC=2BAC, converse *is* true.

The above proof (2(a+c)=f) is used to *solve the following problems:* Q: Prove that in a circle, a chord subtends **equal** angles at any two points on the same one of the two arcs that are determined by the *chord* (Opposite angles in an X style quadrilateral in a circle sum to 180°). Q: The sum of the <u>opposite</u> angles of any quadrilateral inscribed in a circle are together **equal** to 180°. Q: The tangent meeting a triangle in a *circle* problem.

Claim: You can draw a **circle** through any points A,B,C not on a line. Method: draw **perpendicular bisectors** of the sides of the triangles from the vertices. They will meet at the centre of the circumcircle. Drop a *perpendicular* from O to BC. Then $OA^2 = AF^2+OF^2$ (Pythagoras) $= BF^2+OF^2$ (as AF=BF) = OB^2 (Pythagoras) $= OC^2$ *similarly*.

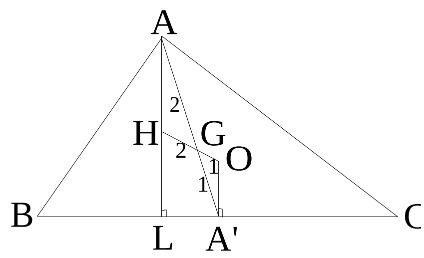


Miguel’s Theorem

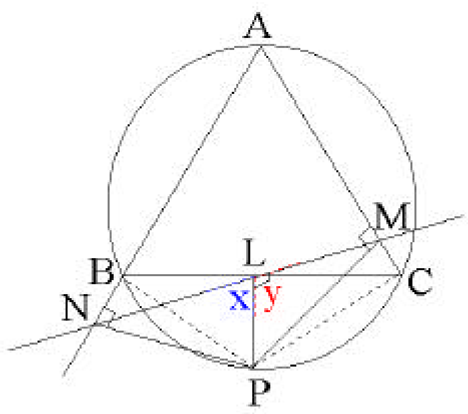


Let L,M,N be points on BC, CA & AB *not coinciding with A,B or C*. Then the circumcircles of AMN, BLN, CLM meet. Proof: Circles BNL, CML meet at a point P, say, i.e. BLPN, CLPM are **cyclic** quadrilaterals. Hence angle NPL = 180° - angle B; Angle LPM = 180° - angle C. Hence angle NPM = 360°-(NPL+LPM) = B+C = 180°-A. Hence NPM, A are *supplementary* (sum to 180°). So A,N,P,M concyclic. So 3 circles meet.

Theorem: The **altitudes** of a triangle are concurrent (Altitude = perpendicular from a vertex to a side. Proof: Let A’ = mid point BC. G divides AA’ in the ratio 2:1. Join OG, **continue** the line to a point H in the ratio 1:2. Join AH to meet BC at L. Consider AHG, OA’G. By proportionality, AH is *parallel* to OA’. AH is perpendicular to BC. The construction of this is independent of the choice of A out of A,B,C. Nice point: Given construction, result is immediate. And get more **information**: O,G,H lie on a straight line.

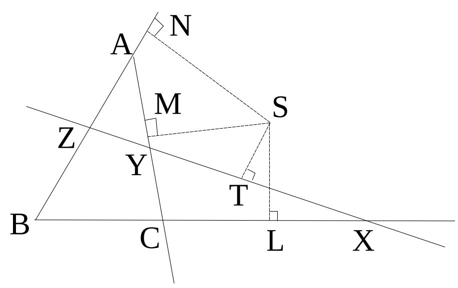


Simson Line



Let P be on the **circumcircle** of ABC. P to BC, CA, AB respectively perpendicular. Then L,M,N is on a straight line. Proof. Required to prove (RTP) x+y=180°. But x = NLP by definition = NBP (because of *right angles* at M,L,N ensure B,N,P,L are concyclic) = 180°-PBA (N,P,A on a straight line) = PCA (Because A,B,C,P are concyclic) = 180°-PLM (P,C,M,L concyclic) = 180°-y by definition. So x+y = 180°. Interested in converse? **Suppose** A,B,C is a triangle. P = point, L,M,N are feet of perpendiculars from P to BC, CA, AB respectively. Then if L,M,N are collinear then A,B,C,P are concyclic. Proof: Reverse above argument. Given x+y=180° in the notation of the above proof, then we deduce that PCA = 180°-PBA (Other parts used right angles at L,M,N). This *implies the* 4 points P,B,C,A are concyclic.

Consider this figure of 4 lines. Each has a circumcircle. Claim: These meet at P. **Proof**: The circumcircles of ABC & AYZ meet at S, say. Drop perpendiculars from S to the four lines. Since S is on the circumference on ABC, the feet of the *perpendiculars* from S to the sides are **collinear** (Simson line from P to ABC).

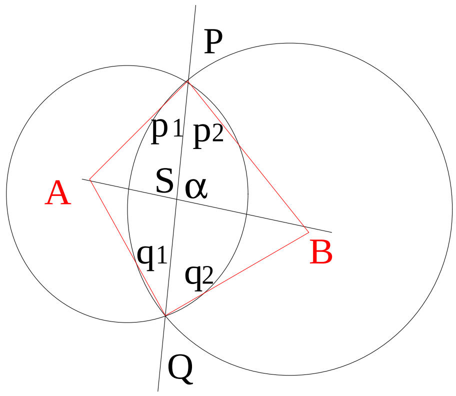


Since S is on the **circumcircle** of AYZ, the feet of the perpendiculars from S once again form a straight line i.e. N,M,T are collinear. So L,M,N,T *lie on a line* using both of the above.

Assignment 1

To prove that the **lines** from the Miguel point to the marked points make equal angles with the sides, label the angles and use *cyclic quadrilaterals* to prove the result. You can construct an infinity of triangles LMN for which S is the Miguel point. Pick an L on AB, then the angle SLB will determine the points M and N (i.e. therefore the angles SNC and SMA will have to be the same as SLB from question 1). All of these *triangles* are similar: when we change the position of L on AB, all we are doing is **changing** the angle SLB. Therefore the other angles SNC and SMA will have to change by the same amount. Hence the Miguel triangles are all similar.

Prove that the line **joining** the centres of two intersecting circles is at right angles to the common chord. Proof: Length BP = length BQ. So $p_2 = q_2$. Because BPQ is isosceles, *similarly* $p_1 = q_1$. Triangles PAB and AQB are congruent (have equal sides). We therefore know angles APB and AQB are equal. This is because APB = p_1+p_2 and AQB = q_1+q_1 (These 2 equations are the same because $q_1=p_1$ and $p_2=q_2$). If the above is **true**, then PBS = SBQ and QAS = PAS. For these two to be the same, because they lie on a straight line, they **must** each be 90°. Therefore $\alpha = 90°$.



Q: Prove that if S is the **Miguel point** for the three points L,M,N on the interiors of the sides of the triangle A,B,C, then the centres of the Miguel triangles form a triangle similar to triangle ABC. A: Use the proof *above and cyclic quadrilaterals*, and this is simple. Q: Consider the figure of 4 lines and their corresponding **4** circumcircles all meeting at a point S. Prove that the centres of these circles also lie *on a circle through S*. A: Let the circumcentres of ABC, AYZ, BZX and CXY be O, O_1, O_2 and O_3. Let O_2O_3 meet SX at X'. Use the **proof** above. Construct similarly B', C' from OO_2, SB; OO_3, SC. Prove X',B',C' are **collinear** (by proving it is parallel to the side of the triangle). Use the *converse of the Simson* line proof to prove that S lies on the circumcircle of OO_2O_3. Now use 1,2 and then 3,1 in place of 2,3. Using all this we can say that the conjecture is correct.

Rounding up: There are only 5 regular solids: *Tetrahedron, Cube, Octahedron (8 equilateral triangles), Dodecahedron (12 pentagons), Icosohedron (20 equilateral triangles).* Each face is a regular polygon (all the same!) At each **vertex** we have the same number of faces. This was the first classification theorem in maths. In Euclid's postulates, he included what is now called the parallel axiom: There exists exactly one line through a point P not on a line *l*, which is parallel to *l*. Many mathematicians tried to **deduce** this from the others, and failed. Finally, in the 19th century, Gauss (privately) & Rolyai. Lobatchesky constructed non-Euclidean geometries, a blow to the idea of geometries being *absolute truths*. We now have the modern ideas of "many geometries", some of which are useful for modelling **aspects** of the real world.

Higher Dimensions

It is easy to **need** many dimensions e.g. a graphic equaliser with 6 knobs. Intuition: moving a *point* creates a line (1). Moving the *line* creates a square (2). Moving a *square* creates a cube (3).... Mathematicians use **many** dimensions e.g. 4, 47. Why? The mathematical notion of space is to describe motion, or of change of data. Data is often structured. To analyse waves e.g. sound waves, you need an **infinite** dimensional space. 4-D Euclidean space (x,y,z,w), all real numbers. 27-D: There exists a special sphere packing leading to a special *error correcting code* used in HDD, CD, Signals.

C(n,r)	0	1	2	3	4	5
0 points	1	2	4	8	16	32
1 edges	0	1	4	12	32	80
2 squares	0	0	1	6	24	80
3 cubes	0	0	0	1	8	40
4 tesseracts	0	0	0	0	1	10

Let C(n,r) be the **number** of r faces of an n-dimensional cube. Where do we start? C(0,0) = 1, or even better, C(-1,r) = 0 and C(n,-1) = 0. *What* is a "-1" cube: A: There aren't any - so the **last** numbers are 0. The formula for the *table* is: C(n+1, r) = 2C(n,r) + C(n, r-1). Geometrically, this says that the r-faces of an n-cube come from **duplicating** the n-cube, and moving the (n-1) faces in the new direction.

Define a *polynomial* $C_n(x) = \sum_{r=0}^{n} C(n,r)x^r$. $C_0(x) = 1$; $C_1(x) = 2+x$; $C_2(x) = 4+4x+x^2 = (2+x)^2$; $C_3(x) = 8+12x+6x^2+x^3 = (2+x)^3$. **Expectation**: $C_n(x) = (2+x)^n$.

The General Idea of New Dimensions

Move from a list $(x_1,...,x_n)$ of n *numbers to a list* $(x_1,...,x_n,x_{n+1})$ of n+1 numbers. Consider the **figures** f (polygons, solids). Each figure f in $\mathbf{R}^n$ is just a set of points. Moving a figure f in $\mathbf{R}^n$ through the new dimension means considering points $(x_1,...,x_n)$ where these vary in f (I) and I^2, the new dimension.

Binomial Theorem: $(a+b)^n = a^n + na^{n-1}b + {}^{n(n-1)}/_{2!}\times a^{n-1}b^2 + ... + nab^{n-1} + b^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$. $\binom{n}{r}$ is also written as ${}^nC_r = {}^{n!}/_{r!(n-r)!}$. **Basic** rule: $\binom{n+1}{r} = \binom{n}{r}+\binom{n}{r-1}$. Also $\binom{n}{r}$ is the *number* of ways of choosing r elements from a set of n elements. Picking out a **coefficient** of x^r in an answer. e.g. in $(2+2x-3x^2)(3+x)^{17} = (2+2x-3x^2)\sum \binom{17}{r} x^r 3^{17-r}$. Pick out the **coefficient** of x^r in the answer: this is given by $2[\sum^{17}_{r=0} \binom{17}{r} x^r 3^{17-r}] + 2x[\sum^{17}_{r=0} \binom{17}{r-1} x^{r-1} 3^{17-(r-1)}] - 3x^2[\sum^{17}_{r=0} \binom{17}{r-2} x^{r-2} 3^{17-(r-2)}]$. **Coefficient** of x^r is $2\binom{17}{r}3^{17-r} + 2\binom{17}{r-1}3^{17-(r-1)} - 3\binom{17}{r-2}3^{17-(r-2)}$.

Assignment 2

	T^2	T^3	T^4
points	3	6	12
edges	3	9	24
faces	1	5	19
3-faces	0	1	7
4-faces	0	0	1

Let T^2 be a triangle. Determine the number of *points, edges and faces of* T^3 when T^2 is moved at right angles into a **new** dimension. This is done with the **table** shown. The same formula T(x+1,r) = 2T(n,r) + T(n,r-1) applies here. Let $t_n(x) = \sum^{n}_{r=0} T(n,r)x^r$. Thus $t_2(x) = 3+3x+x^2$. By more *substitution* and *multiplication*, we deduce that $t_n(x) = (2+x)^{n-2}(3+3x+x^2)$.

By the **Binomial** theorem, $(2+x)^{n-2} = \sum^{n-2}_{r=0} \binom{n-2}{r} 2^{n-2-r}x^r$. So $(3+3x+x^2)(2+x)^{n-2}$ has coefficient of x^r **given** by $3\binom{n-2}{r}2^{n-2-r} + 3\binom{n-2}{r-1}2^{n-1-r} + \binom{n-2}{r-2}2^{n-r}$. The **Euler-Poincare** formula concerns the sum $\sum^{n-1}_{r=0} (-1)^r T(n,r)$ for the **boundary faces** of T^n, or $\sum^{n}_{r=0} (-1)^r T(n,r)$ if we **include** the top-dimensional face. So for T^2, we get 3-3=0. For T^3, we get 6-9+5=2. For T^4, we get 12-24+19-7=0.

Now $t_n(-1) = \sum^{n}_{r=0} (-1)^r T(n,r)$. And *also* $t_n(-1) = (3+3x+x^2)(2+x)^{n-2}$ from which we deduce $t_n(-1)=1$. Hence we **always** have $\sum^{n-1}_{r=0} (-1)^r T(n,r) = 1-(-1)^n = 2$ if n is **odd**, and 0 if n is **even**. This *explains* our results.

General Notes

When drawing, use **perspective**. Geometry about *space*: rotating an electron through 360° gives opposite spin. Another 360° restores the spin. A rotation line in free-space is **described** by the space of a Mobius band & disk with edges glued. Cannot sew a disc to a *mobius* band in 3-dimensions (can in 4). Non-Euclidean geometry: Euclid laid down **axioms** and **postulates** for space — believed to be self-evident truths. But the 5th postulate is equivalent to Playfair's axiom: Given a line *l* and point p on *l*, There exists 1 line through P not meeting *l* i.e. *parallel* to *l*. Early in the 19th century, **Gauss**, **Boleyan** and **Lobotchesky** constructed geometries not satisfying this — geometry on a sphere: no *parallel* lines on a sphere.

Spherical Geometry: People studied plane geometry to help with *agriculture and architecture*. Geometry on a sphere was helpful for navigation. **Erastheres** first estimated the circumference of the Earth. Archimedes had a sphere **inscribed** in a cylinder on his gravestone. Mercator is associated with the map *based on the model* described above. John Harrison's clocks solved the problem of longitude.

The **"great** circle distance" is the name of the shortest distance between two points on the Earth. 2 great circles meet in 2 points. A plane through the **centre** of the sphere cuts the sphere into two equal halves, and meets the sphere in a great circle. This circle has a radius R equal to that of the sphere. Every line of longitude *is half of a great circle*. Two points on a sphere determine precisely **one** great circle through them unless they are anti polar.

Lunes. A lune on a sphere is the region between *2 great circles*. The angle of the lune is the angle between the two great circles. Which angle makes the **lune** a hemisphere? 180°. The area of a sphere is $4\pi r^2$ where r is the radius of the sphere. How does the **area** of the lune depend on its angle? $A = {}^{\alpha°}/_{360°} \times$ area of sphere.

Spherical triangles. Consider a triangle on a sphere with *vertices C* at the north pole and A and B at the equator. What are the **angles** of the triangle at A & B? 90°, 90°. The sum of the angles of the triangle is more than 180°. How is the area of the triangle *related* to the sum of the angles — proportional to α. Can you **find** a triangle will all of its angles right angles? Yes, take $\alpha = 90°$.

Archimedes rule for the **area** of a slice of a sphere. The area of the strip between 2 lines of latitude if the same as the *corresponding area on the surrounding cylinder*. Final remarks: There are **other** geometries: in one of them the world we deal with is the *interior* of a fixed circle D, and a straight line is a portion of a circle which **meets** this fixed circle at right angles. In this geometry, called *hyperbolic*, angle sums in a triangle are less than 180°, a pentagon can have <u>all</u> of its angles as right angles, and many other *mysteries* occur. These strange geometries discovered or invented by the mathematician have a way of **appearing** in new and strange applications. This one turns up in the geometry of the <u>Universe</u>.

<u>T. Porter</u>

If **n** random lines are drawn in the plane, how many *regions* does one get? There is a formula for this, $r_{n+1} = r_n+s_{n+1}$, where s = dimension, r = number of **regions**. Logical questions e.g. "Knights always tell the truth, Knaves lie". So what are the *following* people in the questions. (i) Person A is asked **"Are you a knight**" He answers **"If I am a Knight then I'll eat my hat"**. Does A have to eat his hat? (ii) Two people, A and B, are encountered by the questioner. A says **"If B is a Knight then I am a Knave"**. *What* are A and B?

<u>Proofs and the Algebra of Sets</u>

"$x \in X$" means x **is an** element of X. "$x \notin X$" means x **is not an** element of X. Certain sets have *special* symbols. Examples: Œ = the set of <u>natural</u> numbers {0,1,2,...}. **Z** = the set of <u>integers</u> {...,-2,-1,0,1,2,....}. The **order** is not part of a specification in a list. So {1,3,5,7} is the **same** as {5,1,7,3}. We write ϕ for the **empty** set.

Equality: **2 sets are equal** if they contain precisely the *same* elements. X=Y means $x\in X$ if and only if $x\in Y$. Subset: If every member of Y is a **member** of X, we say that Y is a subset of X and write $Y \subseteq X$. If Y is *not equal* to X, we may write $Y \subset X$. Strategy for proving "$Y \subseteq X$": Let $y \in Y$, ... then $y \in X$. Proof **strategy** for proving "Y=X": Prove $Y\subseteq X$ and then $X\subseteq Y$.

Union: If $X,Y\subseteq U$, then $X\cup Y = \{a: a\in X \text{ or } a\in Y\}$. **Intersection**: If $X,Y\subseteq U$, then $X\cap Y = \{a: a\in X \text{ and } a\in Y\}$. **Complement**: If $X\subseteq U$, $X^c = \{a: a \in U \text{ and } a \notin X\}$. The **algebra** of sets: $\cap$, $\cup$ and $(\ )^c$ interact nicely, satisfying some algebraic *rules*. (see below)

Q: Prove $X\cup(Y\cup Z) \subseteq (X\cup Y)\cup Z$. A: If $x\in X\cup(Y\cup Z)$ **then** either $x\in X$ or $x\in Y\cup Z$. We handle the two possibilities <u>*separately*</u>. (i) If $x\in X$ then $x\in X\cup Y$. This provides the **necessary** argument. As $x\in X\cup Y$, then $x\in (X\cup Y)\cup Z$ (same "lemma" used again). (ii) if $x\in Y\cup Z$ then *either* $x\in Y$ or $x\in Z$. If $x\in Y$ then $x\in X\cup Y$ and **hence** in $(X\cup Y)\cup Z$. If $x\in Z$, then $x\in (X\cup Z)\cup Z$. In both cases we use the same idea as before: $X\subset X\cup Y$. We should **next** prove $(X\cup Y)\cup Z \subseteq X\cup(Y\cup Z)$. But since this is almost the same, we just say similarly we have $(X\cup Y)\cup Z \subseteq X\cup(Y\cup Z)$. There is a *similar* proof for $(X\cap Y)\cap Z = X\cap(Y\cap Z)$.

For **any** sets X,Y and Z (Subsets of U), we have the following rules shown on the <u>next</u> page...

(1) $X \cap X = X$. (2) $X \cup X = X$. (3) $X \cap X^c = \phi$. (4) $X \cup X^c = U$. (5) $X \cap Y = Y \cap X$ and $X \cup Y = Y \cup X$. (6) $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ and $X \cup (Y \cup Z) = (X \cup Y) \cup Z$. (7) $(X \cap Y)^c = X^c \cup Y^c$ and $(X \cup Y)^c = X^c \cap Y^c$. (8) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ and $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. (9) $(X^c)^c = x$. (10) $X \cap \phi = \phi$. (11) $X \cup \phi = X$. (12) $X \cap U = X$ and $X \cup U = U$. (13) $X \cap (X \cup Y) = X$ and $X \cup (X \cap Y) = X$.

Define X\Y as "X take away Y", $X \setminus Y = \{z: z \in X \text{ and } z \notin Y\}$. This gives $X \setminus Y = X \cap Y^c$. But \ is not associative, so that $X \setminus (Y \setminus Z)$ is not equal to $(X \setminus Y) \setminus Z$. Looking at the subsets of $X = \{a_1, a_2, a_3)$, we have $8 = 2^3$ subsets. More **generally**, if we have n elements, then we have 2^n subsets. Looking at the set $2 = \{0,1\}$, if X is a set and $A \subseteq X$, we define a function $\chi_A: X \rightarrow 2$. We set $\chi_A(x) = 1$ if $x \in A$ and $\chi_A(x) = 0$ if $x \notin A$. This function χ_A is called the **characteristic** *function* of A.

If A and B are **subsets** of X, then they have the *same characteristic function* iff they are equal sets. Every **function** from X to 2 is the characteristic function of some subset of X. If X is a set, the set of functions from X to 2 is written 2^X. Recall that the set of subsets of X is called the power set and is written P(X). The function $\chi: P(X) \rightarrow 2^X$ given by sending the subset A to its characteristic function χ_A is a <u>one-to-one</u> function.

<u>Assignment 3</u>

Define an operation $\vee$ on 2 by defining $a \vee b = 1$ if either $a=1$ or $b=1$, and is 0 otherwise. If f and g are functions *from X to 2*, we **define** $f \vee g$ by $(f \vee g)(x) = f(x) \vee g(x)$. So to get the $\vee$ of two functions, you just $\vee$ the **images** of each point. If A and B are *subsets* of X, then $\chi_A \vee \chi_B = \chi_{A \cup B}$.

Define a new **operation**: $a \Delta b = 0$ if $a+b$ is even and 1 if $a+b$ is odd. This "**addition**" is associative (For any a,b,c in 2, $(a \Delta b) \Delta c = a \Delta (b \Delta c)$). As before, we **extend** the operation to the functions from X to 2 by defining $f \Delta g$ as $(f \Delta g)(x) = f(x) \Delta g(x)$. If X is a **set** and A and B are subsets of X, define the *symmetric difference* $A \Delta B = (A \setminus B) \cup (B \setminus A)$. In other words, $A \Delta B$ is the set {z: $z \in A$ or $z \in B$, but not in both}. If A and B are **subsets** of X, prove that $\chi_A \Delta \chi_B = \chi_{A \Delta B}$. Using the **characteristic** functions we can prove that $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

Applying the characteristic function on $(A \Delta B) \Delta C$, first on $(A \Delta B)$, $(\chi_{A \Delta B}) \Delta C$. But we know that $\chi_{A \Delta B} = \chi_A \Delta \chi_B$, so we have $(\chi_A \Delta \chi_B) \Delta C$. Now applying the **characteristic** function on $(\chi_A \Delta \chi_B) \Delta C$, in the form $(A) \Delta B$, $(\chi_A \Delta \chi_B) \Delta \chi_C$. But for **characteristic function values**, we have already proved that $(a \Delta b) \Delta c = a \Delta (b \Delta c)$. So we can say that because $(a \Delta b) \Delta c = a \Delta (b \Delta c)$, then we have $(\chi_A \Delta \chi_B) \Delta \chi_C = \chi_A \Delta (\chi_B \Delta \chi_C)$. **Hence** $(A \Delta B) \Delta C = A \Delta (B \Delta C)$. QED.

<u>De Morgan's Laws</u>

Proof of $(X \cap Y)^c \subseteq X^c \cup Y^c$. Suppose that $x \in (X \cap Y)^c$, then $x \notin X \cap Y$. So either $x \notin X$ or $x \notin Y$. If $x \notin X$ then $x \in X^c$, so $x \in X^c \cup Y^c$. If $x \in Y$ then $x \in Y^c$ and again $x \in X^c \cup Y^c$. So if $x \in (X \cap Y)^c$ then $x \in X^c \cup Y^c$ so $(X \cap Y)^c \subseteq X^c \cup Y^c$. *We can prove* "the other way around" similarly. Note: To prove $(X \cup Y)^c \subseteq X^c \cap Y^c$, we use the <u>substitution</u> $A = X^c$ and $B = Y^c$. Try it!

Functions

Functions allow us to **compare** sets. They are essential in *applications* of sets. Several proof strategies are used in studying functions. What is a function? A function f from a set X to a set Y is an **assignment** to each element x of X an element of Y, denoted f(x), called the image of x. X is the *domain* of f; Y is the *codomain* of f. We write f: X→Y.

A function may be specified by a **formula, diagram, table or inductively/recursively** e.g. f(n) = 2f(n-1) yields f(n) = 2^n. Special types of *function*: f is one-to-one (or injective) if for x,x'∈X, f(x) = f(x') implies x=x'. (No 2 district elements of X have the same image in Y). Useful formula in manipulation: $\frac{x^n - x'^n}{x - x'} = \sum x^k x^{n-k-1}$. f is onto (or **surjective**) if for any y∈Y, there is some x∈X with f(x) = y. If f is injective and surjective, it is bijective.

In X = {1,2,3} and f: X→Y, we only have *bijections* or *nothing*. The number of bijections is 6 = 3!. **Cardinality**. Definition: Two sets X and Y have the same cardinality, written |X| = |Y|, if there is a bijection from X to Y. If |X| = |{1,2,...,n}| we **say that** |X| = n. If there is a 1-to-1 function f: X→Y, then |X| ≤ |Y|. If X and Y are finite then this is easy to say; if infinite it is really a definition. If there is no bijection from X to Y, then |X| < |Y|.

Russell's Paradox is an example of another proof strategy: proof by contradiction. You assume the *opposite* of what you want to prove, and deduce some obvious falsehood or contradiction. As the original statement could not be false, it **must** therefore be true. We will see proof by contradiction several times e.g. in proving that √2 is not a rational number.

Relations

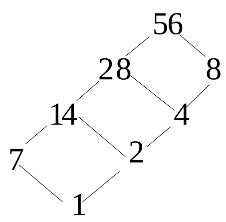
Let X and Y be sets. A relation R from X to Y is a **subset** of the set X×Y of ordered pairs, {(x,y): x∈X, y∈Y}. If (x,y)∈**R** we write xRy and say x is related to y. If X=Y we say R is a relation on X. Most **examples** will have X=Y. Properties of *relations*. Let R be a relation on a set X. (i) R is said to be reflexive if for all x∈X, xRx (i.e. every **element** is related to itself). (ii) R is *symmetric* if for all x,y∈X, xRy implies yRx. (iii) R is weakly anti-symmetric if for all x,y∈X, if xRy and yRx then x=y. (iv) R is *transitive* if ∀ x,y,z∈X, if xRy and yRz, then xRz.

Examples: Let X = DIV_{36} = {1,2,3,4,6,9,12,18,36}, the set of divisors of 36. Write x|y if x divides y exactly (for x,y ∈ DIV_{36}) so 2|12 but 2 not| 9. (1) **Reflexive**? Yes. Any x∈DIV_{36} divides itself, x|x. (2) **Symmetric**? No! 2|4 but 4 not| 2. (3) **Weakly anti-symmetric?** Yes — there are reciprocals. (4) **Transitive**? Yes!

Tutorial

|X∪Y| = |X|+|Y| for **disjoint** sets. For non-disjoint sets, |X∪Y| = |X|+|Y|-|X∩Y|. For three sets, |X∪Y∪Z| = |X|+|Y|+|Z| - |X∩Z| - |X∩Y| - |X∩Y| + |X∩Y∩Z|. These expressions can be *proved* by using Venn diagrams. A relation is called an equivalence relation if it is reflexive, symmetric and transitive. A relation is called a partial order relation if it is reflexive, weakly anti-symmetric and transitive.

A **Hasse** diagram for such a partial order is a diagram in which each element of the set is represented by a *vertex*, and an edge is drawn (upwards) from x to y if x < y (and there are no elements z strictly between x and y). For **instance**, the Hasse diagram for the divisors of 56 is as shown. You can create Hasse diagrams for e.g. the ordered set $(P(X), \subseteq)$, where $X = \{1,2,3,4\}$.



Proofs and Logic

Propositions are "**sentences**" that have a definite truth value (true, t, or false, f). Operators: (All are shown below in the table) (1) *Negation*. We write $\neg p$ for the negation of p. (2) **Disjuction** (OR). $p \vee q$ is true **exactly** if at least one of p and q is true. (3) **Conjunction** (AND): $p \wedge q$ is true exactly when **both** p and q are true.

p	**q**	**$\neg p$**	**$p \wedge q$**	**$p \vee q$**	**$p \Rightarrow q$**
t	t	f	t	t	t
t	f	f	f	t	f
f	t	t	f	t	t
f	f	t	f	f	t

We can build up **compound propositions, terms, or boolean expressions** by combining these operators. For example, $p = (q \wedge r) \vee (r \wedge \neg s)$. **Implication**. When is $p \Rightarrow q$ true? The key to filling in the table is a "rule of deduction", MODUS PONENS, which tells us how we expect $\Rightarrow$ ("implies") to react. If we know that $p \Rightarrow q$ is true, and that p is true, then we expect to **deduce** that q is true. In other words, $(p \wedge (p \Rightarrow q)) \Rightarrow q$ should always be **true** (a tautology). Both the *bottom* entries would be "t" i.e. $p \Rightarrow q$ is only false when p is **true** and q is **false**. This has implication for *proof*. Example: If you want to **prove** that $p \Rightarrow q$ is false, then just find one *example* where p is true and q is false.

Assignment 4

Use **truth tables** to analyse if expressions are equivalent ($\Leftrightarrow$). We can check whether a *boolean expression* is reflexive, weakly anti-symmetric ("up to equivalence") and transitive. They can be e.g. **partial order** relations. To check as above, use the technique shown below, or truth tables. All *boolean* expressions can be expressed as a **single** connective, NOR. NOR, with symbol $\downarrow$, is defined as $(\neg p) \wedge (\neg q)$. We can find expressions such as $\neg p$, $p \vee q$ and $p \wedge q$ **solely** in terms of the NOR operator.

TRANSITIVE

$(p \leq r) \wedge (r \leq q) \Rightarrow p \leq q$

$((p \Rightarrow r) \wedge (r \Rightarrow q)) \Rightarrow p \leq q$

$((p \Rightarrow r) \wedge (r \Rightarrow q)) \Rightarrow (p \Rightarrow q)$

f

t f

t f t f

t ? ? f t f

Technique to show *something is true*. To show that something is a tautology, assume it **isn't** and proceed as shown. For the example shown, $p \leq q$ is specified exactly when $(p \vee q) \Leftrightarrow q$ is true. We want to prove that the symbol $\leq$ is *transitive*. In the bottom line, we've already **decided** on the values of p & q by the RHS of the expression (p=t and q=f is the only way that the RHS is false). But no matter **what** we choose for r, we cannot make the LHS true *without r being inconsistent*. So the expression is **always** true (a tautology).

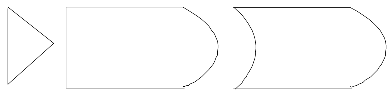
The Algebra of Propositions

The **following** are *logical identities:* (1) $(p\wedge q)\Leftrightarrow p$. (2) $(p\vee p)\Leftrightarrow p$. (3) $(p\wedge \neg p)\Leftrightarrow f$. (4) $(p\vee \neg p)\Leftrightarrow t$. (5) $(p\wedge q)\Leftrightarrow(q\wedge p)$. (6) $(p\vee q)\Leftrightarrow(q\vee p)$. (7) $p\wedge(q\wedge r)\Leftrightarrow(p\wedge q)\wedge r$. (8) $p\vee(q\vee r)\Leftrightarrow(p\vee q)\vee r$. (9) $\neg(p\wedge q)\Leftrightarrow \neg p\vee \neg q$. (10) $\neg(p\vee q)\Leftrightarrow \neg p\wedge \neg q$. (11) $p\wedge(q\vee r)\Leftrightarrow(p\wedge q)\vee(p\wedge r)$. (12) $p\vee(q\wedge r)\Leftrightarrow(p\vee q)\wedge(p\vee r)$. (13) $\neg\neg p\Leftrightarrow p$. (14) $(p\Rightarrow q)\Leftrightarrow(\neg q\Rightarrow \neg p)$. This is the <u>contrapositive</u> law. (15) $p\wedge t\Leftrightarrow p$ and $p\vee t\Leftrightarrow t$. (16) $p\wedge f\Leftrightarrow f$ and $p\vee f\Leftrightarrow p$. (17) $p\wedge(p\vee q)\Leftrightarrow p$ and $p\vee(p\wedge q)\Leftrightarrow p$. Note: each can be established by using **truth** tables, but also by algebra — e.g. contrapositive *from what we already know*: $(p\Rightarrow q)\Leftrightarrow \neg(p\wedge \neg q)\Leftrightarrow \neg(\neg(q)\wedge(\neg\neg p)\Leftrightarrow(\neg q\Rightarrow \neg p)$.

Boolean Expressions

p	q	p⇔q
t	t	t
t	f	f
f	t	f
f	f	t

Many **statements** in maths take the form "p if and only if q". These get used to "translate" *one* statement into another (perhaps more usable) equivalent statement. "p iff q" is used to mean "if p then q **and** if q then p". So the <u>notation</u> "⇔" is used. (Truth table as shown). So "$p\Leftrightarrow q$" is thus short for "$(p\Rightarrow q)\wedge(q\Rightarrow p)$". Two propositions that are logically **equivalent** have the same truth table. **Logic Circuits**. Using simple *components* as shown, we can build up circuits to model expressions.



Formal Definitions

"**Ingredients**": set of variables $X = \{x_1,...x_n\}$; symbols *not, and, or, true, false*. Rules for building expressions: **recursive** definition: (i) t,f are boolean expressions; for any $x\in X$, x is a **boolean** expression. (ii) If P is a boolean expression, then so is **not** P. (iii) If P and Q are boolean expressions, so are $P\vee Q$ and $P\wedge Q$. Boolean expressions give *functions*. If P involves the variables $x_1,...x_n$, then we get a function $B^n\rightarrow B$, where $B = \{t,f\}$.

Proposition: Every function from B^n to B can be represented by a *boolean* expression. Proof: Suppose we are given a <u>function</u> $F: B^n\rightarrow B$. Tabulate F (giving a truth table). For each row of $F(x_1,...x_n)$, pick out those rows giving an **output** of t. For each row, form an *expression*

$$q = \bigwedge_{i=1,n} \begin{cases} x_i & \text{if there is a t in the } x_i \text{ column} \\ \neg x_i & \text{if there is an f in the } x_i \text{ column} \end{cases}.$$

Now form $q_1\vee q_2\vee...\vee q_n$, where there are 'k' t's in the output. This **expression** gives the function F. An example is shown in the *table*. For this, $P = q_1\vee q_2$, where $q_1 = x_1\wedge \neg x_2\wedge x_3$ and $q_2 = \neg x_1\wedge x_2\wedge \neg x_3$. So $P = (x_1\wedge \neg x_2\wedge x_3)\vee(\neg x_1\wedge x_2\wedge \neg x_3)$.

x_1	x_2	x_3	**f**
t	t	t	f
t	t	f	f
t	f	t	t
t	f	f	f
f	t	t	f
f	t	f	t
f	f	t	f
f	f	f	f

An **application** of this is a "black box" with *n inputs and 1 output.* Find a **circuit** that gives exactly the desired output. Each input channel is either ON (1 or t) or OFF (0 or f). Plan: (i) Find a *boolean expression modelling the operation* of the "Black Box". (ii) Use the logic circuit ideas sketched earlier to get an **actual** circuit which does the job. (iii) <u>Simplify</u> the expression (if possible) — this we **won't** do.

Exam Paper: January 1999

SECTION 1 (Compulsory)

(1) (a) Give diagrams illustrating two cases of the theorem "The angle at the centre is twice the angle at the circumference", and prove one of these cases. **[4 marks]**

(b) State and prove a converse to your theorem in (a). **[6 marks]**
You are given two facts about subsets of the set X. Firstly for any subset A of X, $(A^c)^c = A$. Secondly for any two subsets B, C of X, $(B \cap C)^c = B^c \cup C^c$. Using these facts and nothing more prove that for any two subsets, D, E of X, $(D \cup E)^c = D^c \cap E^c$. **[5 marks]**

(c) Using a truth table, or otherwise, prove that the following is a tautology.
$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$. **[5 marks]**

SECTION 2 (Answer 2 out of 4 questions)

(2) Let O, O' be the centres of circles meeting in points D, E and let P be the mid of DE. Prove that O, P, O' are colinear. **[6 marks]**

Let ABC be a triangle and let L, M, N be points on BC, CA, AB respectively. Prove that the circles AMN, BNL, CLM have a common point, and that the centres of these circles form a triangle similar to ΔABC. **[9 marks]**

[Any facts on isosceles triangles and cyclic quadrilaterals used should be stated clearly.]

(3) A hexagon H^2 lying in a plane is moved at right angles to the plane through one unit of length, forming a solid figure H^3. Determine the number of points, edges and faces of H^3. Now H^3 is moved in a fourth dimension through one unit of length, forming a figure H^4. Determine the number of points, edges and 2-dimensional faces of H^4. Explain your working clearly. **[7 marks]**

Let H^n be obtained similarly from H^{n-1} for any $n \geq 3$. Let H(n, r) be the number of r-dimensional faces of H^n. Let $h_n(x) = \sum_{r=-1}^{\infty} H(n, r)x^r$. Explain why $h_{n+1}(x) = (x+2)h_n(x)$. Hence find a formula for H(n, r). **[8 marks]**

(4) (a) Suppose f: A→B is a function and T and U are subsets of B.
Define $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$, similarly for $f^{-1}(U)$.

(i) Prove that if $T \subseteq U$ then $f^{-1}(T) \subseteq f^{-1}(U)$. **[5 marks]**

(ii) Give an example of a function f: A→B and subsets T, U of B such that $f^{-1}(T) \subseteq f^{-1}(U)$ but T is not a subset of U. (Hint: Use your favourite function that is not one-to-one.) **[5 marks]**

(b) Find the number of onto functions from {1,2,3,4} to {a,b}. You should briefly justify your method of finding them and how you know you have the exact number. **[5 marks]**

(5) (a) You are given n random lines in the plane ‘ ^{2} and these divide the plane into r_n regions. Prove that $r_{n+1} = r_n+(n+1)$. **[7 marks]**
[Lines are ‘random’ if no two are parallel and no three meet in a point.]

(b) You are given n random planes in 3 dimensional space ‘ ^{3}. These divide ‘ ^{3} into ρ_n regions. Prove that $\rho_{n+1} = \rho_n+r_n$. **[8 marks]**

[Planes are ‘randomly placed’ if no two are parallel, no three meet in a line and no four meet in a point.]

(Questions done: 1, 2, 3)